# ENCRYPTION POLICY

**MISIXS, LLC**
**Version 1.1 - Approved by GRC**
**Effective Date: January 2, 2026**

## Contents


1. Objective
2. Scope
3. Policy Statement
4. Encryption at Rest
5. Encryption in Transit
6. Password Encryption
7. Cryptographic Key Management
8. Document Security Classification
9. Non-Compliance
10. Responsibilities
11. Schedule
12. Version History


## 1. Objective

Encryption is a process in which data is encoded so that it remains hidden from or inaccessible to unauthorized users. It helps protect private data, sensitive information, and can enhance the security of communication between client apps and servers.

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that encryption is used appropriately and in compliance with applicable regulations and best practices.

This policy supports MISIXS, LLC's commitment to implement reasonable administrative, technical, and organizational measures designed to protect Personal Data as described in the Data Processing Agreement.

## 2. Scope

This policy applies to all MISIXS, LLC staff members, contractors, service providers, and subprocessors who work with or have access to MISIXS systems and data.

This policy covers:

- All brands, products, and services offered under MISIXS, LLC, including the RuleFirst platform and any other current or future branded offerings operating under any "doing business as" or similar trade names
- All data at rest (stored data) and data in transit (transmitted data)
- All systems, applications, databases, and infrastructure used to provide the Platform and Services
- All Customer Data and Personal Data processed on behalf of customers
- All MISIXS proprietary and confidential information

## 3. Policy Statement

### 3.1 General Encryption Requirements

MISIXS, LLC requires that all sensitive data, including Personal Data and Customer Data, be protected through appropriate encryption controls both at rest and in transit.

MISIXS implements reasonable administrative, technical, and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Encryption is a critical technical control supporting this commitment.

### 3.2 Algorithm Requirements

Cryptographic algorithms used for encryption shall be well-established, publicly vetted, and approved by recognized standards bodies such as NIST (National Institute of Standards and Technology).

Staff members and developers shall not implement custom or proprietary encryption algorithms. If there is a business need for a custom encryption approach, it must be escalated to the Information Security Officer at privacy@misixs.com for review and approval.

## 4. Encryption at Rest

Encryption at rest refers to the encryption of data while it is stored on a device or system. This includes data stored in databases, file systems, backups, and any other storage media.

### 4.1 Managed Databases

All managed databases (e.g., AWS RDS, Azure SQL Database, Google Cloud SQL) shall have encryption at rest enabled using the infrastructure provider's native encryption capabilities.

Database encryption shall use industry-standard algorithms such as AES-256 (Advanced Encryption Standard with 256-bit keys).

### 4.2 Infrastructure Provider Encryption

Where MISIXS uses cloud infrastructure providers (such as AWS, Azure, or Google Cloud Platform), encryption at rest shall be enabled for all storage services including:

- Object storage (e.g., AWS S3, Azure Blob Storage, Google Cloud Storage)
- Block storage (e.g., AWS EBS, Azure Managed Disks)
- File storage systems
- Backup and archive storage

### 4.3 Endpoint Encryption

All laptops, desktops, and mobile devices used by MISIXS staff members that store or access sensitive data shall have full-disk encryption enabled.

Endpoint encryption requirements are detailed in the Endpoint Security Policy (if available) or the Acceptable Usage Policy.

## 5. Encryption in Transit

Encryption in transit refers to the encryption of data while it is being transmitted over networks, including internal networks and the public internet.

### 5.1 HTTPS and TLS Requirements

All web applications, APIs, and services provided by MISIXS shall use HTTPS with SSL/TLS encryption enabled.

The minimum acceptable TLS version is TLS 1.2. TLS 1.3 is preferred where supported.

Older protocols (SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1) shall not be used due to known security vulnerabilities.

### 5.2 Certificate Requirements

Security certificates shall be provided by known, trusted certificate authorities (CAs) such as Let's Encrypt, DigiCert, or other publicly trusted CAs.

Self-signed certificates shall not be used in production environments unless specifically approved by the Information Security Officer for internal-only systems.

Certificates shall be monitored for expiration and renewed before expiry to prevent service disruptions.

### 5.3 API and Service-to-Service Communication

All API endpoints shall require HTTPS/TLS encryption.

Service-to-service communication within MISIXS infrastructure shall use encrypted channels where technically feasible.

### 5.4 Email Encryption

Email transmission shall use TLS encryption where supported by the recipient's mail server.
Sensitive information sent via email should be encrypted or transmitted through secure file-sharing systems when possible.

## 6. Password Encryption

Passwords shall never be stored in plaintext.
All passwords shall be hashed using industry-standard, cryptographically secure hashing algorithms such as:

- bcrypt
- scrypt
- Argon2
- PBKDF2 with appropriate iteration counts

Passwords shall be salted before hashing to prevent rainbow table attacks.
Legacy hashing algorithms such as MD5 and SHA-1 shall not be used for password storage.

## 7. Cryptographic Key Management

Cryptographic keys used for encryption shall be managed securely throughout their lifecycle, including generation, storage, distribution, rotation, and destruction.

### 7.1 Key Generation

Cryptographic keys shall be generated using cryptographically secure random number generators.
Key generation shall follow industry best practices and use appropriate key lengths (e.g., AES-256, RSA-2048 or higher).

### 7.2 Key Storage

Encryption keys shall be stored separately from the data they protect.
Keys shall be stored in secure key management systems (KMS) such as AWS KMS, Azure Key Vault, or HashiCorp Vault where available.
Keys shall not be hard-coded in application source code or configuration files.

### 7.3 Key Rotation

Encryption keys shall be rotated periodically in accordance with industry best practices and regulatory requirements.
Key rotation schedules shall be documented and followed consistently.

### 7.4 Key Access Control

Access to encryption keys shall be restricted to authorized personnel and systems only.
Key access shall be logged and monitored for unauthorized access attempts.

### 7.5 Key Destruction

When encryption keys are no longer needed, they shall be securely destroyed in accordance with industry best practices.
Key destruction shall be documented and auditable.

## 8. Document Security Classification

Company Internal (please refer to the Data Classification Policy for more details, if available).

## 9. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, security assessments, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

## 10. Responsibilities

The designated Information Security Officer or equivalent role is responsible for approving and reviewing this policy. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

**Specific Responsibilities:**

- **Information Security Officer:** Overall authority for encryption policy, standards, and compliance
- **Engineering and Development Teams:** Implementation of encryption controls in applications and systems
- **Infrastructure and Operations Teams:** Configuration and maintenance of encryption for infrastructure and data storage
- **All Staff Members:** Compliance with encryption requirements when handling sensitive data

**Contact Information:**

For encryption policy questions, technical guidance, and approval requests:

**Email:** privacy@misixs.com

**Mailing Address:** MISIXS, LLC 970 Nolder Drive Lancaster, Ohio 43130 United States

## 11. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization, technology infrastructure, or regulatory requirements.

## 12. Version History

| Version | Status | Log | Date |
|---|---|---|---|
| 1.1 | Current | Initial policy version for MISIXS, LLC | January 2, 2026 |

**END OF ENCRYPTION POLICY**